

# ENROLLED

COMMITTEE SUBSTITUTE

FOR

## H. B. 4316

---

(BY DELEGATES M. POLING, PERRY, MOYE,  
TOMBLIN, YOUNG, BARRETT, BARILL, WALKER,  
PASDON, PETHTEL AND FRAGALE)

---

[Passed March 8, 2014; in effect ninety days from passage.]

AN ACT to amend the Code of West Virginia, 1931, as amended, by adding thereto a new section, designated §18-2-5h, relating to creating the student data accessibility, transparency and accountability act; providing definitions; state, district and school responsibilities for data inventory; providing for data governance manager and responsibilities; establishing parental rights to information and providing for policies on security and access; requiring state board rules; and establishing effect on existing data.

*Be it enacted by the Legislature of West Virginia:*

That the code of West Virginia, 1931, as amended, be amended by adding thereto a new section, designated §18-2-5h, to read as follows:

**ARTICLE 2. STATE BOARD OF EDUCATION.**

**§18-2-5h. Student Data Accessibility, Transparency and Accountability Act.**

1           (a) *Title.* — This section shall be known and may be cited as  
2 the “Student Data Accessibility, Transparency and Account-  
3 ability Act.”

4           (b) *Definitions.* — As used in this section, the following  
5 words have the meanings ascribed to them unless the context  
6 clearly implies a different meaning:

7           (1) “Board” means the West Virginia Board of Education;

8           (2) “Department” means the West Virginia Department of  
9 Education;

10          (3) “Student Data system” means the West Virginia  
11 Department of Education statewide longitudinal data system;

12          (4) “Aggregate data” means data collected that is reported at  
13 the group, cohort, or institutional level with a data set of  
14 sufficient size that no information for an individual parent or  
15 student is identifiable;

16 (5) “Redacted data” means a student dataset in which parent  
17 and student identifying information has been removed;

18 (6) “State-assigned student identifier” means the unique  
19 student identifier assigned by the state to each student that shall  
20 not be or include the Social Security number of a student in  
21 whole or in part;

22 (7) “Student data” means data collected or reported at the  
23 individual student level included in a student’s educational  
24 record;

25 (8) “Provisional student data” means new student data  
26 proposed for inclusion in the student data system;

27 (9) “School district” means a county board of education, the  
28 West Virginia Schools for the Deaf and Blind and the West  
29 Virginia Department of Education with respect to the education  
30 programs under its jurisdiction that are not in the public schools;

31 (10) “Directory information” means the following individual  
32 student information that is subject to disclosure for school-  
33 related purposes only: Student name, address, telephone number,  
34 date and place of birth, major field of study, participation in  
35 officially recognized activities and sports, weight and height of

36 members of athletic teams, dates of attendance, indication of  
37 “graduate” or “non-graduate,” degrees and awards receives, most  
38 recent previous school attended, and photograph.

39 (11) “Confidential student information” means data relating  
40 to a person’s Social Security number, or other identification  
41 number issued by a state or federal agency, except for the state-  
42 assigned student identifier as defined in this section, religious  
43 affiliation, whether the person or a member of their household  
44 owns or possesses a firearm, whether the person or their family  
45 are or were recipients of financial assistance from a state or  
46 federal agency, medical, psychological or behavioral diagnoses,  
47 criminal history, criminal history of parents, siblings or any  
48 members of the person’s household, vehicle registration number,  
49 driver’s license number, biometric information, handwriting  
50 sample, credit card numbers, consumer credit history, credit  
51 score, or genetic information;

52 (12) “Affective computing” means human-computer  
53 interaction in which the device has the ability to detect and  
54 appropriately respond to its user’s emotions and other stimuli;  
55 and

56 (13) “Fair Information Practice Principles” are United States  
57 Federal Trade Commission guidelines that represent widely  
58 accepted concepts concerning fair information practice in an  
59 electronic marketplace.

60 (c) *Data Inventory – State Responsibilities.* — The  
61 Department of Education shall:

62 (1) Create, publish, and make publicly available a data  
63 inventory and dictionary or index of data elements with  
64 definitions of individual student data fields in the student data  
65 system to include, but not be limited to:

66 (A) Any individual student data required to be reported by  
67 state and federal education mandates;

68 (B) Any individual student data which has been proposed in  
69 accordance with paragraph (A), subdivision (7) of this  
70 subsection for inclusion in the student data system with a  
71 statement regarding the purpose or reason and legal authority for  
72 the proposed collection; and

73 (C) Any individual student data that the department collects  
74 or maintains with no current identified purpose;

75 (2) Develop, publish, and make publicly available policies  
76 and procedures to comply with all relevant state and federal  
77 privacy laws and policies, including, but not limited to, the  
78 Federal Family Educational Rights and Privacy Act (FERPA)  
79 and other relevant privacy laws and policies. The policies and  
80 procedures specifically shall include, but are not limited to:

81 (A) Access to student and redacted data in the statewide  
82 longitudinal data system shall be restricted to:

83 (i) The authorized staff of the department and the contractors  
84 working on behalf of the department who require access to  
85 perform their assigned duties as required by law and defined by  
86 interagency data-sharing agreements;

87 (ii) District administrators, teachers and school personnel  
88 who require access to perform their assigned duties;

89 (iii) Students and their parents; and

90 (iv) The authorized staff of other West Virginia state  
91 agencies as required by law and defined by interagency  
92 data-sharing agreements;

93 (B) Ensure that any inter-agency data-sharing agreements  
94 shall be posted on the Department website, and parents shall be

95 notified of their right to opt out of sharing the child's data  
96 pursuant to agreements.

97 (C) Use only aggregate data in public reports or in response  
98 to record requests in accordance with this section;

99 (D) Unless otherwise prohibited by law, develop criteria for  
100 the approval of research and data requests from state and local  
101 agencies, the Legislature, researchers working on behalf of the  
102 department, and the public. Student data maintained by the  
103 department shall remain redacted; and

104 (E) Notification to students and parents regarding student  
105 privacy rights under federal and state law;

106 (3) Unless otherwise provided by law, the department shall  
107 not transfer student or redacted data that is confidential under  
108 this section to any federal, state or local agency or other  
109 organization, public or private, with the following exceptions:

110 (A) A student transfers out-of-state or a school or school  
111 district seeks help with locating an out-of-state transfer;

112 (B) A student leaves the state to attend an out-of-state  
113 institution of higher education or training program;

114 (C) A student registers for or takes a national or multistate  
115 assessment;

116 (D) A student voluntarily participates in a program for which  
117 a data transfer is a condition or requirement of participation;

118 (E) The department enters into a contract that governs  
119 databases, assessments, special education or instructional  
120 supports with an in-state or out-of-state contractor for the  
121 purposes of state level reporting;

122 (F) A student is classified as “migrant” for federal reporting  
123 purposes; or

124 (G) A federal agency is performing a compliance review.

125 (4) Develop a detailed data security plan that includes:

126 (A) Guidelines for the student data system and for  
127 individual student data including guidelines for authentication of  
128 authorized access;

129 (B) Privacy compliance standards;

130 (C) Privacy and security audits;

131 (D) Breach planning, notification and procedures;

132 (E) Data retention and disposition policies; and

133 (F) Data security policies including electronic, physical, and  
134 administrative safeguards, such as data encryption and training  
135 of employees;

136 (5) Ensure routine and ongoing compliance by the  
137 department with FERPA, other relevant privacy laws and  
138 policies, and the privacy and security policies and procedures  
139 developed under the authority of this act, including the  
140 performance of compliance audits;

141 (6) Ensure that any contracts that govern databases,  
142 assessments or instructional supports that include student or  
143 redacted data and are outsourced to private vendors include  
144 express provisions that safeguard privacy and security and  
145 include penalties for noncompliance; and

146 (7) Notify the Governor and the Legislature annually of the  
147 following:

148 (A) New student data proposed for inclusion in the state  
149 student data system. Any proposal by the Department of  
150 Education to collect new student data must include a statement  
151 regarding the purpose or reason and legal authority for the  
152 proposed collection. The proposal shall be announced to the

153 general public for a review and comment period of at least sixty  
154 days and approved by the state board before it becomes effective.  
155 Any new student data collection approved by the state board is  
156 a provisional requirement for a period sufficient to allow schools  
157 and school districts the opportunity to meet the new requirement;

158 (B) Changes to existing data collections required for any  
159 reason, including changes to federal reporting requirements made  
160 by the U.S. Department of Education and a statement of the  
161 reasons the changes were necessary;

162 (C) An explanation of any exceptions granted by the state  
163 board in the past year regarding the release or out-of-state  
164 transfer of student or redacted data; and

165 (D) The results of any and all privacy compliance and  
166 security audits completed in the past year. Notifications  
167 regarding privacy compliance and security audits shall not  
168 include any information that would itself pose a security threat  
169 to the state or local student information systems or to the secure  
170 transmission of data between state and local systems by exposing  
171 vulnerabilities.

172           (8) Notify the Governor upon the suspicion of a data security  
173 breach or confirmed breach and upon regular intervals as the  
174 breach is being managed. The parents shall be notified as soon  
175 as possible after the suspected or confirmed breach.

176           (9) Prohibit the collection of confidential student  
177 information as defined in subdivision ten of subsection (b) of this  
178 section.

179           (d) *Data Inventory – District Responsibilities.* — A school  
180 district shall not report to the state the following individual  
181 student data:

- 182           (1) Juvenile delinquency records;
- 183           (2) Criminal records;
- 184           (3) Medical and health records; and
- 185           (4) Student biometric information.

186           (e) *Data Inventory – School Responsibilities.* — Schools  
187 shall not collect the following individual student data:

- 188           (1) Political affiliation and beliefs;
- 189           (2) Religion and religious beliefs and affiliations;
- 190           (3) Any data collected through affective computing;

191 (4) Any data concerning the sexual orientation or beliefs  
192 about sexual orientation of the student or any student's family  
193 member; and

194 (5) Any data concerning firearm's ownership by any member  
195 of a student's family.

196 (f) *Data Governance Manager*. — The state superintendent  
197 shall appoint a data governance manager, who shall report to and  
198 be under the general supervision of the state superintendent. The  
199 data governance manager shall have primary responsibility for  
200 privacy policy, including:

201 (1) Assuring that the use of technologies sustain, and do not  
202 erode, privacy protections relating to the use, collection, and  
203 disclosure of student data;

204 (2) Assuring that student data contained in the student data  
205 system is handled in full compliance with the Student Data  
206 Accessibility, Transparency, and Accountability Act, FERPA,  
207 and other state and federal privacy laws;

208 (3) Evaluating legislative and regulatory proposals involving  
209 collection, use, and disclosure of student data by the Department  
210 of Education;

211 (4) Conducting a privacy impact assessment on proposed  
212 rules of the state board and department in general and on the  
213 privacy of student data, including the type of personal  
214 information collected and the number of students affected;

215 (5) Coordinating with the general counsel of the state board  
216 and department, other legal entities, and organization officers to  
217 ensure that programs, policies, and procedures involving civil  
218 rights, civil liberties, and privacy considerations are addressed in  
219 an integrated and comprehensive manner;

220 (6) Preparing a report to the Legislature on an annual basis  
221 on activities of the department that affect privacy, including  
222 complaints of privacy violations, internal controls, and other  
223 matters;

224 (7) Establishing department-wide policies necessary for  
225 implementing Fair Information Practice Principles to enhance  
226 privacy protections;

227 (8) Working with the Office of Data Management and  
228 Analysis, the general counsel, and other officials in engaging  
229 with stakeholders about the quality, usefulness, openness, and  
230 privacy of data;

231 (9) Establishing and operating a department-wide Privacy  
232 Incident Response Program to ensure that incidents are properly  
233 reported, investigated and mitigated, as appropriate;

234 (10) Establishing and operating a process for parents to file  
235 complaints of privacy violations;

236 (11) Establishing and operating a process to collect and  
237 respond to complaints of privacy violations and provides redress,  
238 as appropriate; and

239 (12) Providing training, education and outreach to build a  
240 culture of privacy across the department and transparency to the  
241 public.

242 The data governance manager shall have access to all  
243 records, reports, audits, reviews, documents, papers,  
244 recommendations, and other materials available to the  
245 department that relate to programs and operations with respect  
246 to his or her responsibilities under this section and shall make  
247 investigations and reports relating to the administration of the  
248 programs and operations of the department as are necessary or  
249 desirable.

250       (g) *Parental rights regarding child's information and*  
251 *education record.* — Parents have the right to inspect and review  
252 their child's education record maintained by the school and to  
253 request student data specific to their child's educational record.  
254 School districts must provide parents or guardians with a copy of  
255 their child's educational record upon request. Whenever  
256 possible, an electronic copy of the educational record must be  
257 provided if requested and the identity of the person requesting  
258 the information is verified as the parent or guardian.

259       The state board shall develop guidance for school district  
260 policies that:

261       (1) Annually notify parents of their right to request student  
262 information;

263       (2) Ensure security when providing student data to parents;

264       (3) Ensure student data is provided only to the authorized  
265 individuals;

266       (4) Detail the timeframe within which record requests must  
267 be provided;

268       (5) Ensure that school districts have a plan to allow parents  
269 to view and access data specific to their child's educational

270 record and that any electronic access provided is restricted to  
271 eligible parties;

272 (6) Ensure compliance in the collection, use and disclosure  
273 of directory information and providing parents or guardians with  
274 a form to limit the information concerning their child in directory  
275 and subject to release; and

276 (7) Informing parents of their rights and the process for filing  
277 complaints of privacy violations.

278 (h) *State Board Rules.* — The state board shall adopt rules  
279 necessary to implement the provisions of the Student Data  
280 Accessibility, Transparency, and Accountability Act.

281 (i) *Effect on Existing Data.* — Upon the effective date of this  
282 section, any existing student data collected by the Department of  
283 Education shall not be considered a new student data collection  
284 under this section.